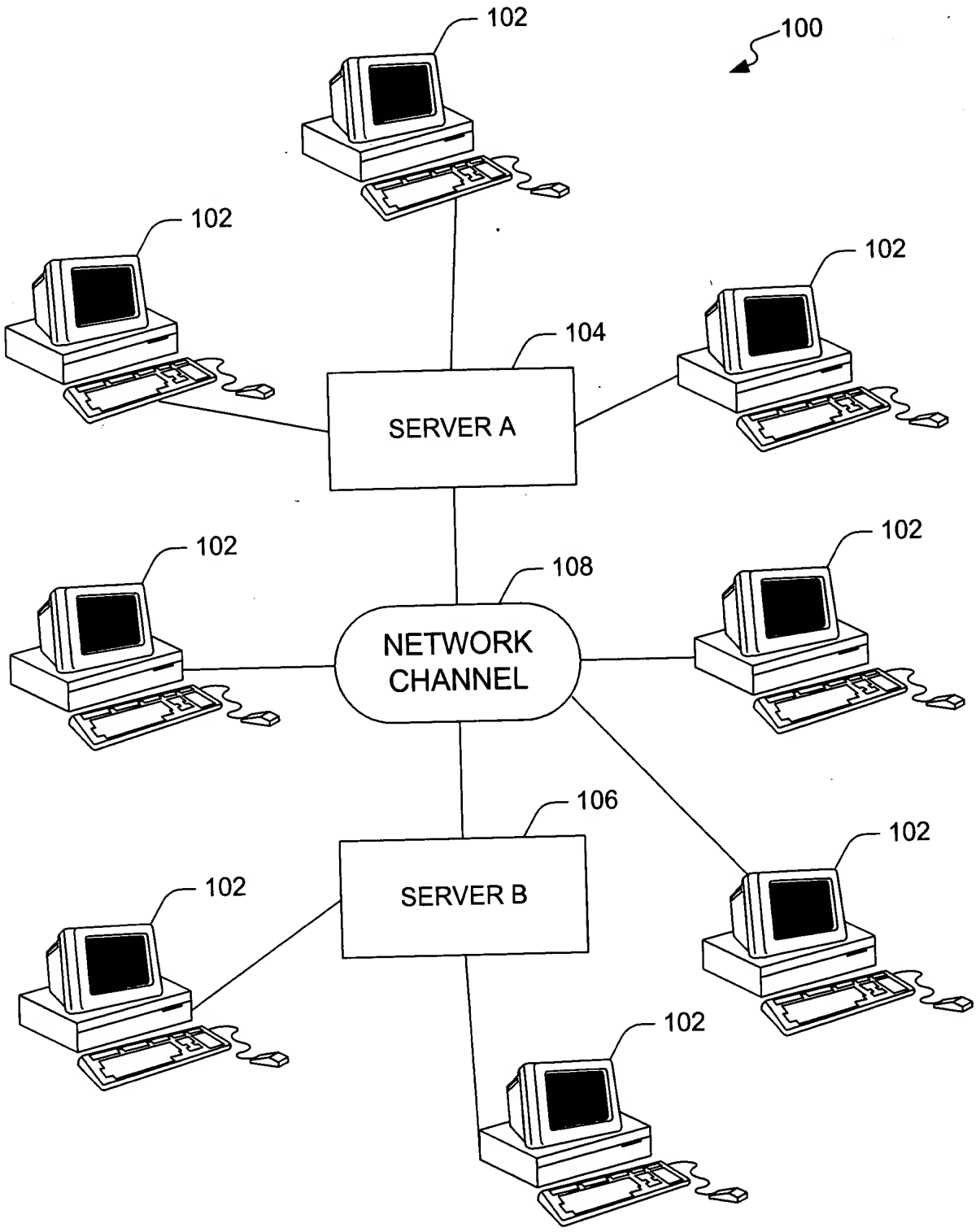
100
102
102
102
104
SERVER A
102
102
108
NETWORK
CHANNEL
102
106
102
SERVER B
102

FIG. 1

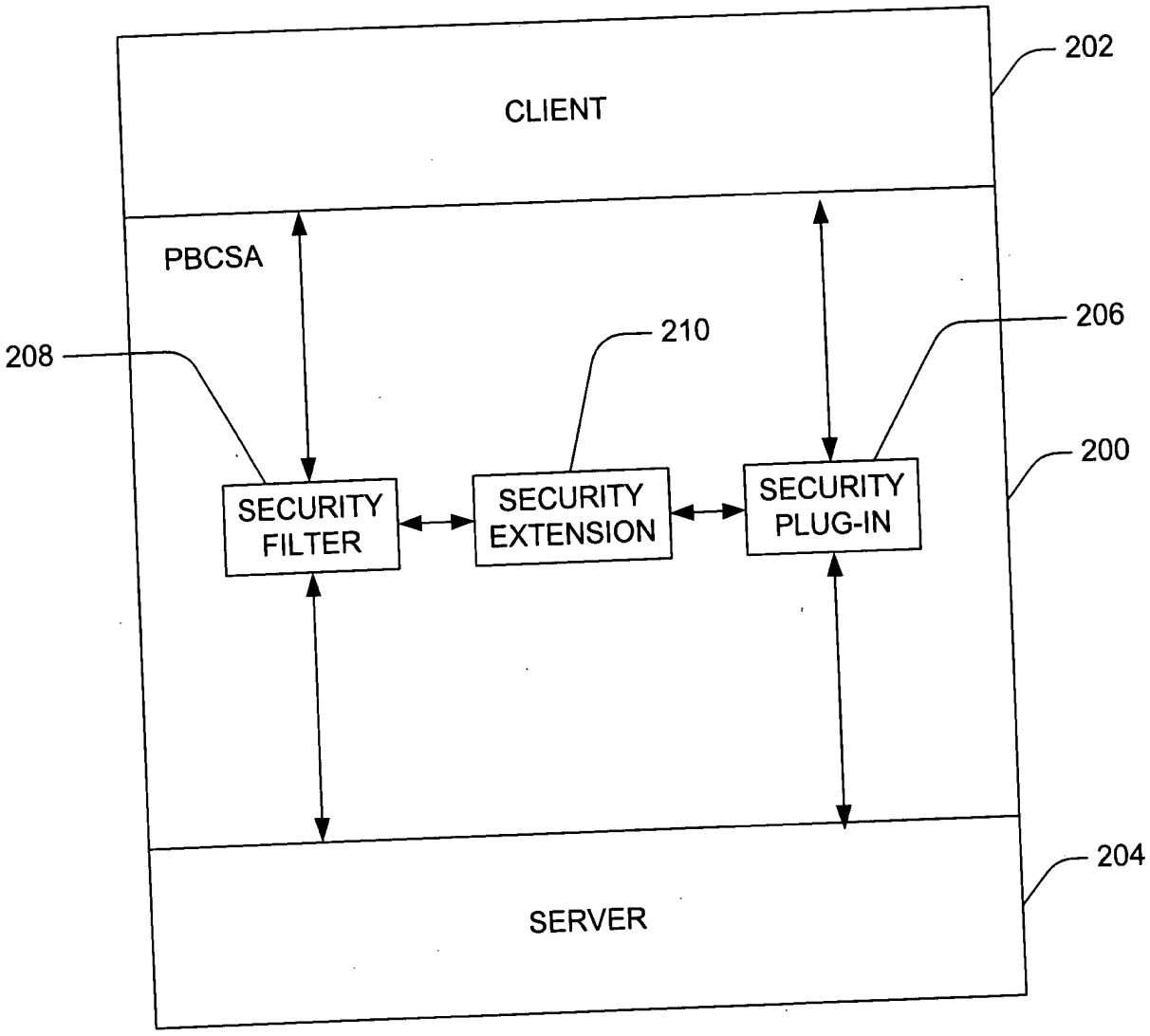
CLIENT
202
PBCSA
208
210
206
200
SECURITY FILTER
SECURITY EXTENSION
SECURITY PLUG-IN
204
SERVER

FIG. 2

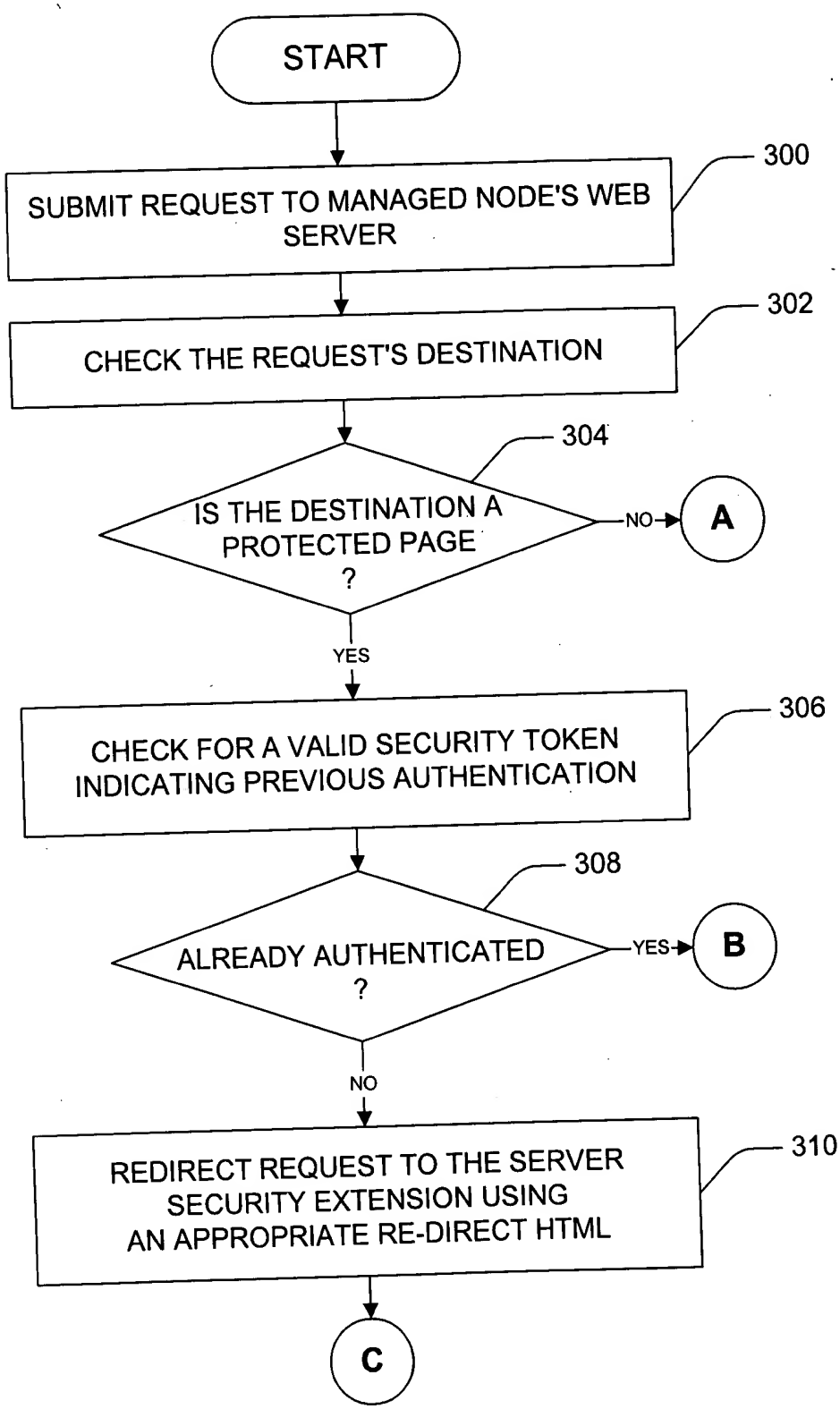
START
SUBMIT REQUEST TO MANAGED NODE'S WEB SERVER
300
CHECK THE REQUEST'S DESTINATION
302
IS THE DESTINATION A PROTECTED PAGE ?
304
NO
A
YES
CHECK FOR A VALID SECURITY TOKEN INDICATING PREVIOUS AUTHENTICATION
306
ALREADY AUTHENTICATED ?
308
YES
B
NO
REDIRECT REQUEST TO THE SERVER SECURITY EXTENSION USING AN APPROPRIATE RE-DIRECT HTML
310
C

FIG. 3A

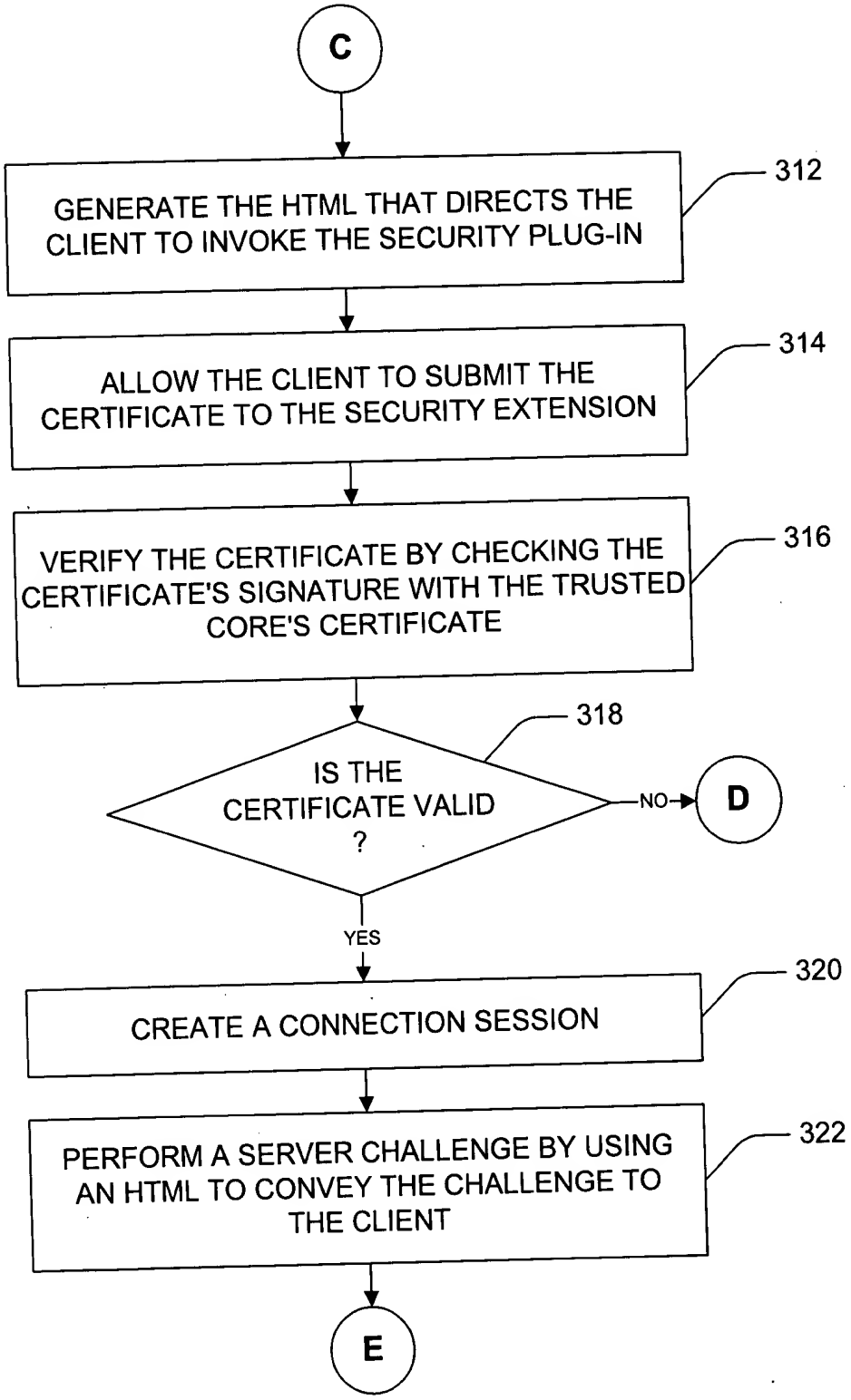
C
GENERATE THE HTML THAT DIRECTS THE CLIENT TO INVOKE THE SECURITY PLUG-IN
312
ALLOW THE CLIENT TO SUBMIT THE CERTIFICATE TO THE SECURITY EXTENSION
314
VERIFY THE CERTIFICATE BY CHECKING THE CERTIFICATE'S SIGNATURE WITH THE TRUSTED CORE'S CERTIFICATE
316
IS THE CERTIFICATE VALID ?
318
NO
D
YES
CREATE A CONNECTION SESSION
320
PERFORM A SERVER CHALLENGE BY USING AN HTML TO CONVEY THE CHALLENGE TO THE CLIENT
322
E

FIG. 3B

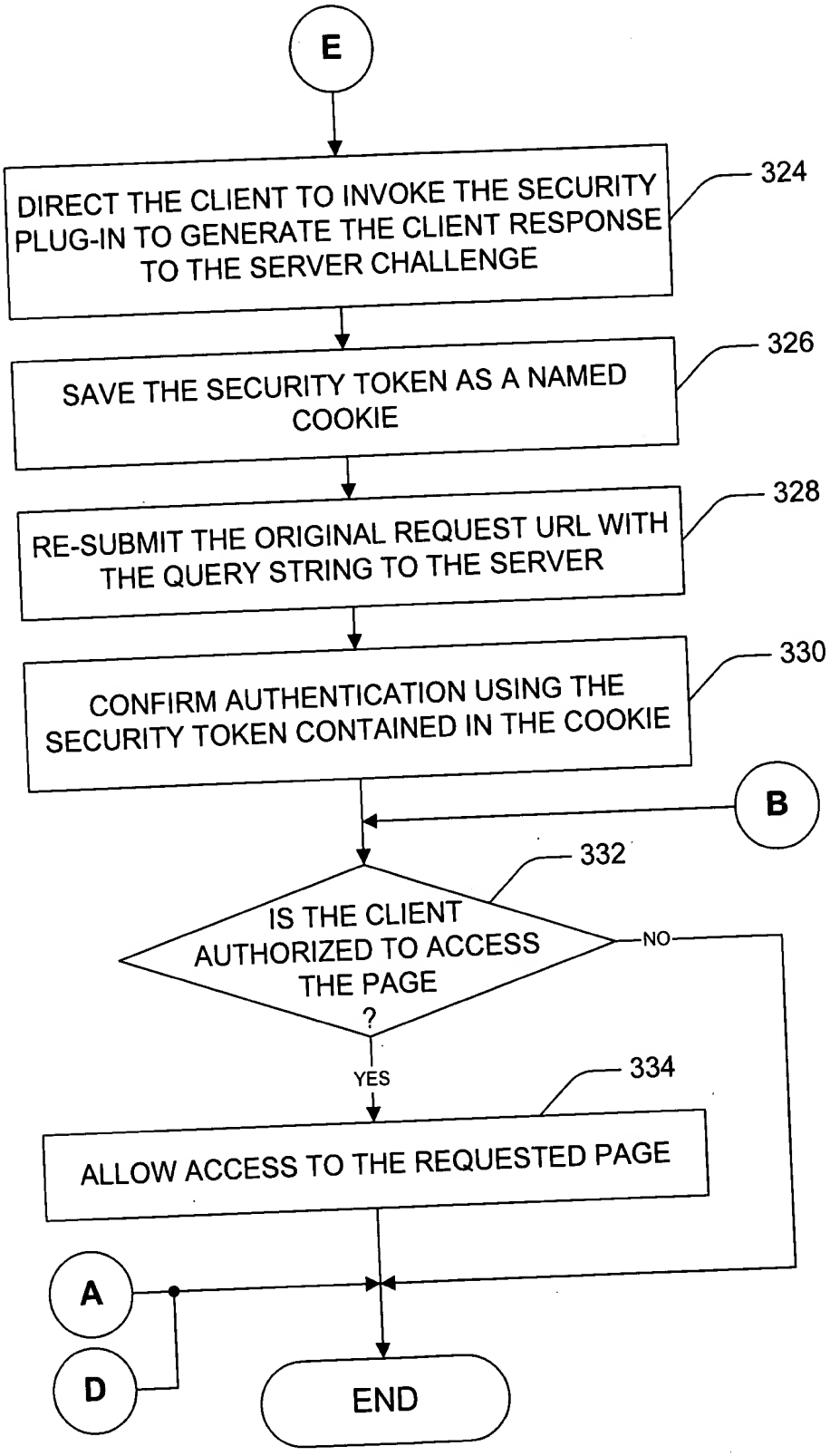
E
DIRECT THE CLIENT TO INVOKE THE SECURITY PLUG-IN TO GENERATE THE CLIENT RESPONSE TO THE SERVER CHALLENGE
324
SAVE THE SECURITY TOKEN AS A NAMED COOKIE
326
RE-SUBMIT THE ORIGINAL REQUEST URL WITH THE QUERY STRING TO THE SERVER
328
CONFIRM AUTHENTICATION USING THE SECURITY TOKEN CONTAINED IN THE COOKIE
330
B
332
IS THE CLIENT AUTHORIZED TO ACCESS THE PAGE ?
NO
YES
334
ALLOW ACCESS TO THE REQUESTED PAGE
A
D
END

FIG. 3C

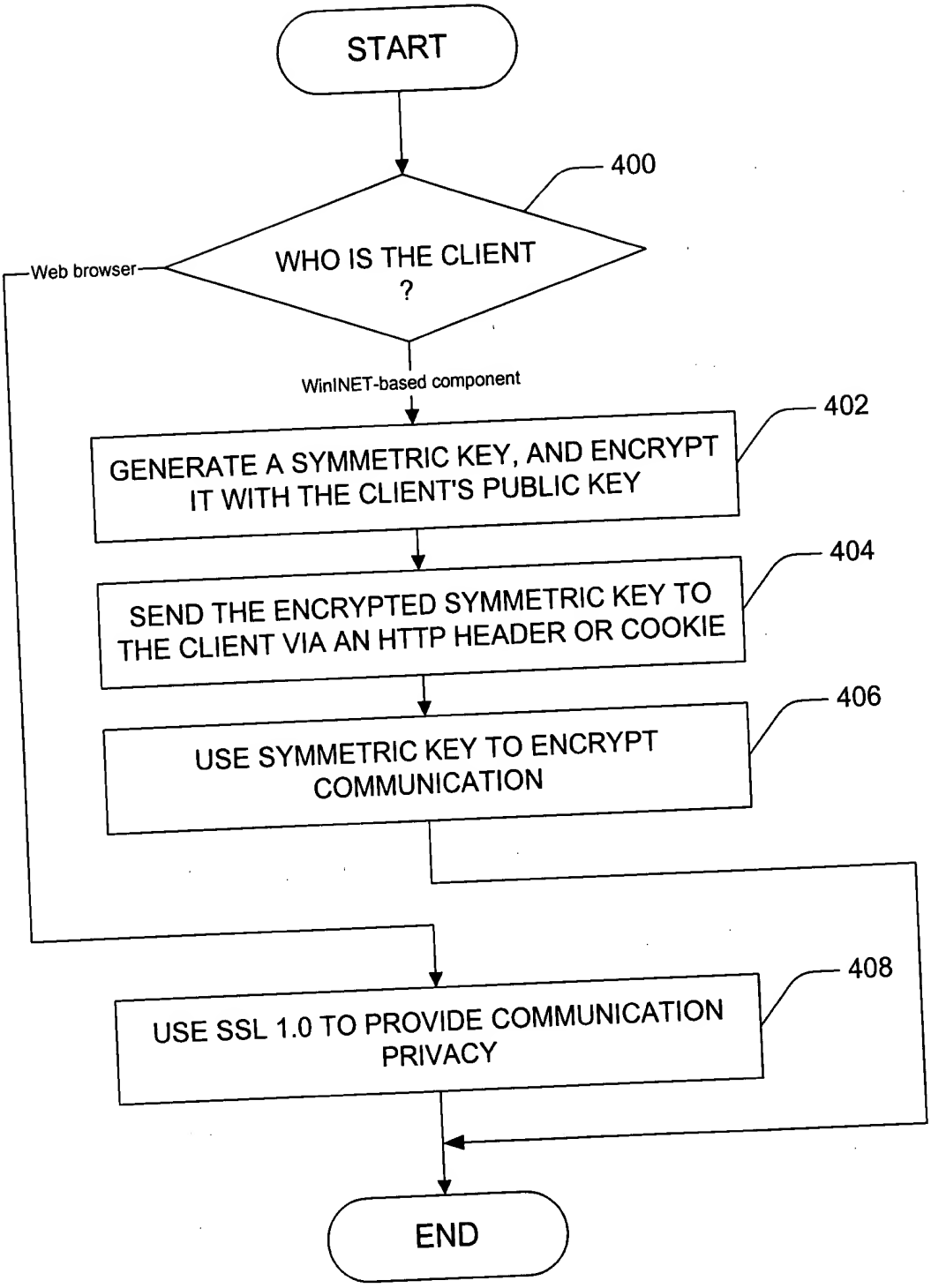
START
400
WHO IS THE CLIENT ?
Web browser
WinINET-based component
402
GENERATE A SYMMETRIC KEY, AND ENCRYPT IT WITH THE CLIENT'S PUBLIC KEY
404
SEND THE ENCRYPTED SYMMETRIC KEY TO THE CLIENT VIA AN HTTP HEADER OR COOKIE
406
USE SYMMETRIC KEY TO ENCRYPT COMMUNICATION
408
USE SSL 1.0 TO PROVIDE COMMUNICATION PRIVACY
END

FIG. 4

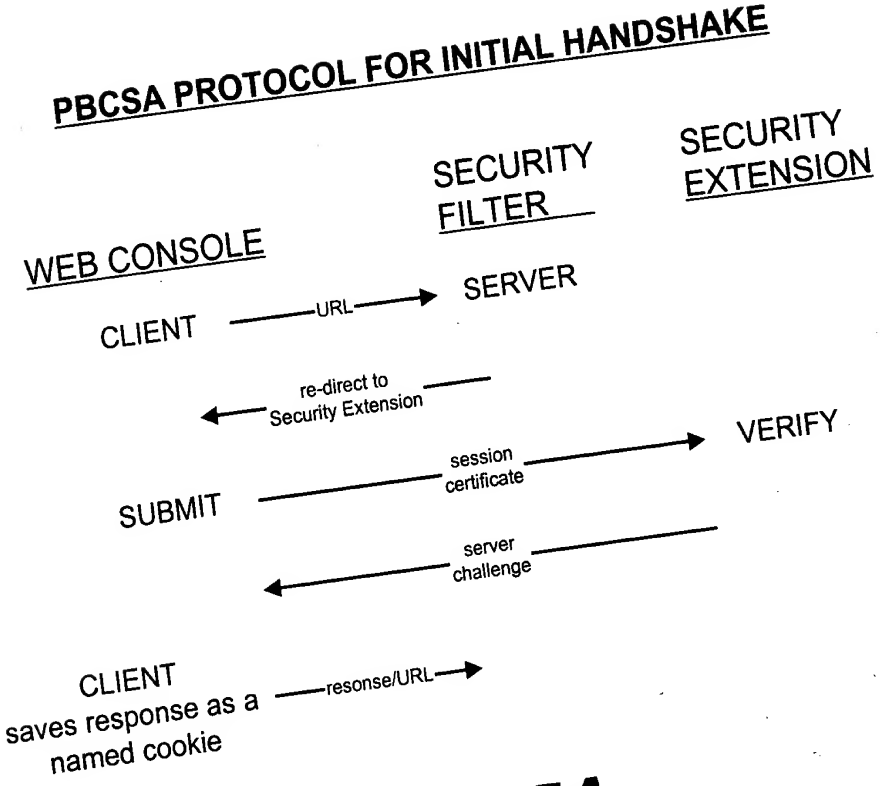


FIG. 5A

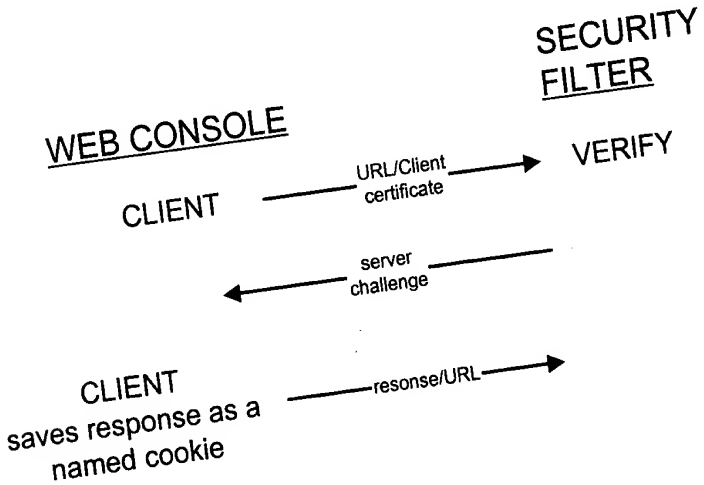


FIG. 5B

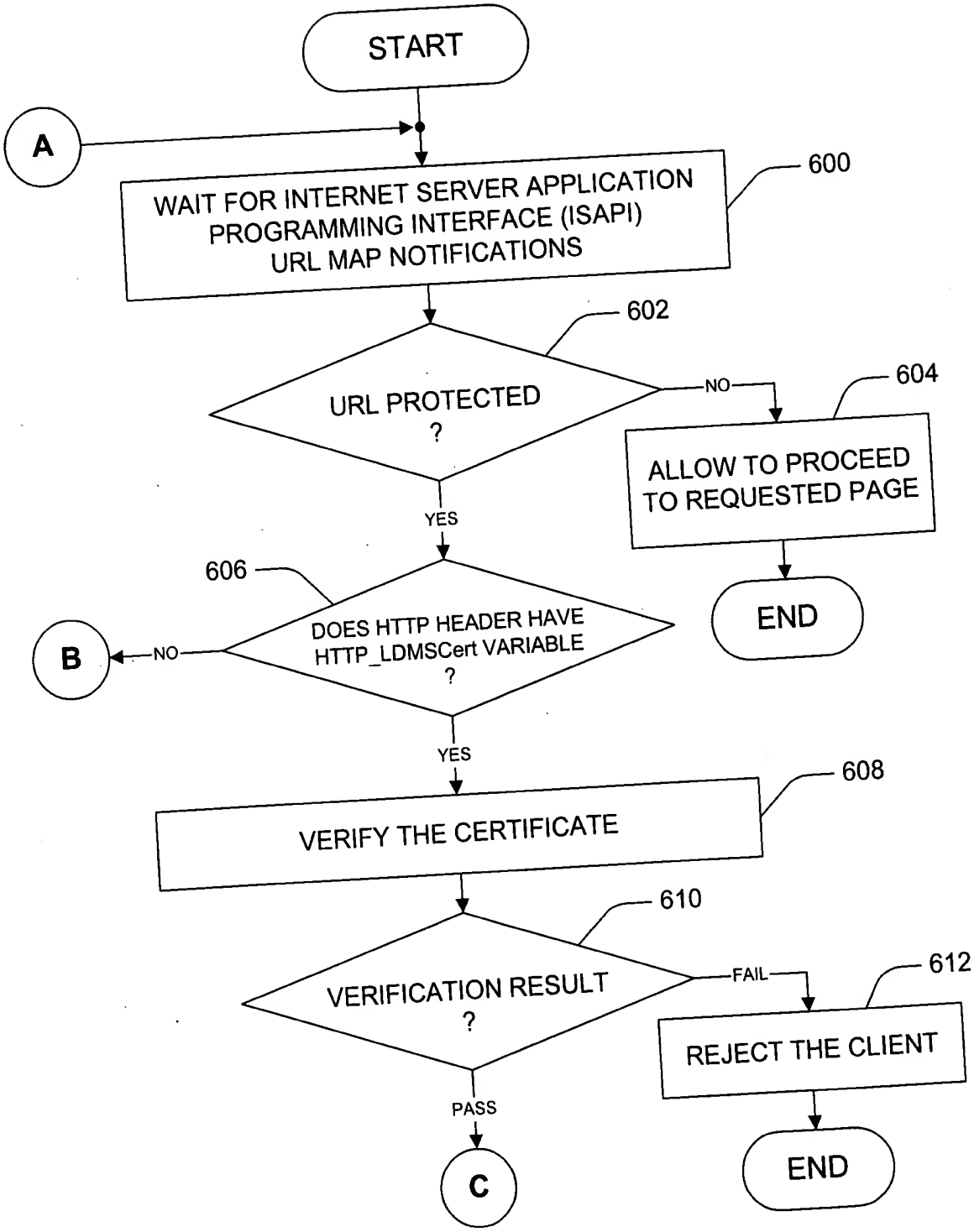
START
A
WAIT FOR INTERNET SERVER APPLICATION PROGRAMMING INTERFACE (ISAPI) URL MAP NOTIFICATIONS
600
602
URL PROTECTED ?
NO
604
ALLOW TO PROCEED TO REQUESTED PAGE
END
YES
606
DOES HTTP HEADER HAVE HTTP_LDMSCert VARIABLE ?
B
NO
YES
608
VERIFY THE CERTIFICATE
610
VERIFICATION RESULT ?
FAIL
612
REJECT THE CLIENT
END
PASS
C

FIG. 6A

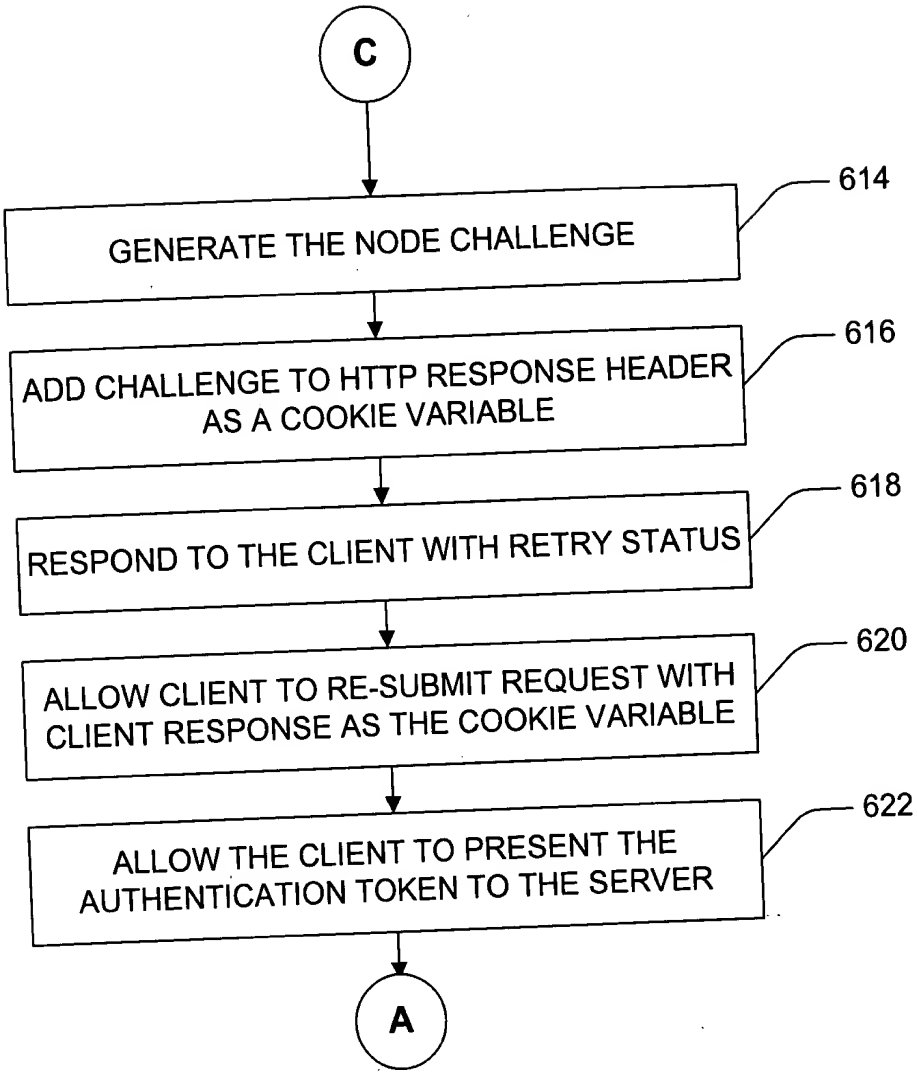
C
GENERATE THE NODE CHALLENGE
614
ADD CHALLENGE TO HTTP RESPONSE HEADER AS A COOKIE VARIABLE
616
RESPOND TO THE CLIENT WITH RETRY STATUS
618
ALLOW CLIENT TO RE-SUBMIT REQUEST WITH CLIENT RESPONSE AS THE COOKIE VARIABLE
620
ALLOW THE CLIENT TO PRESENT THE AUTHENTICATION TOKEN TO THE SERVER
622
A

FIG. 6B

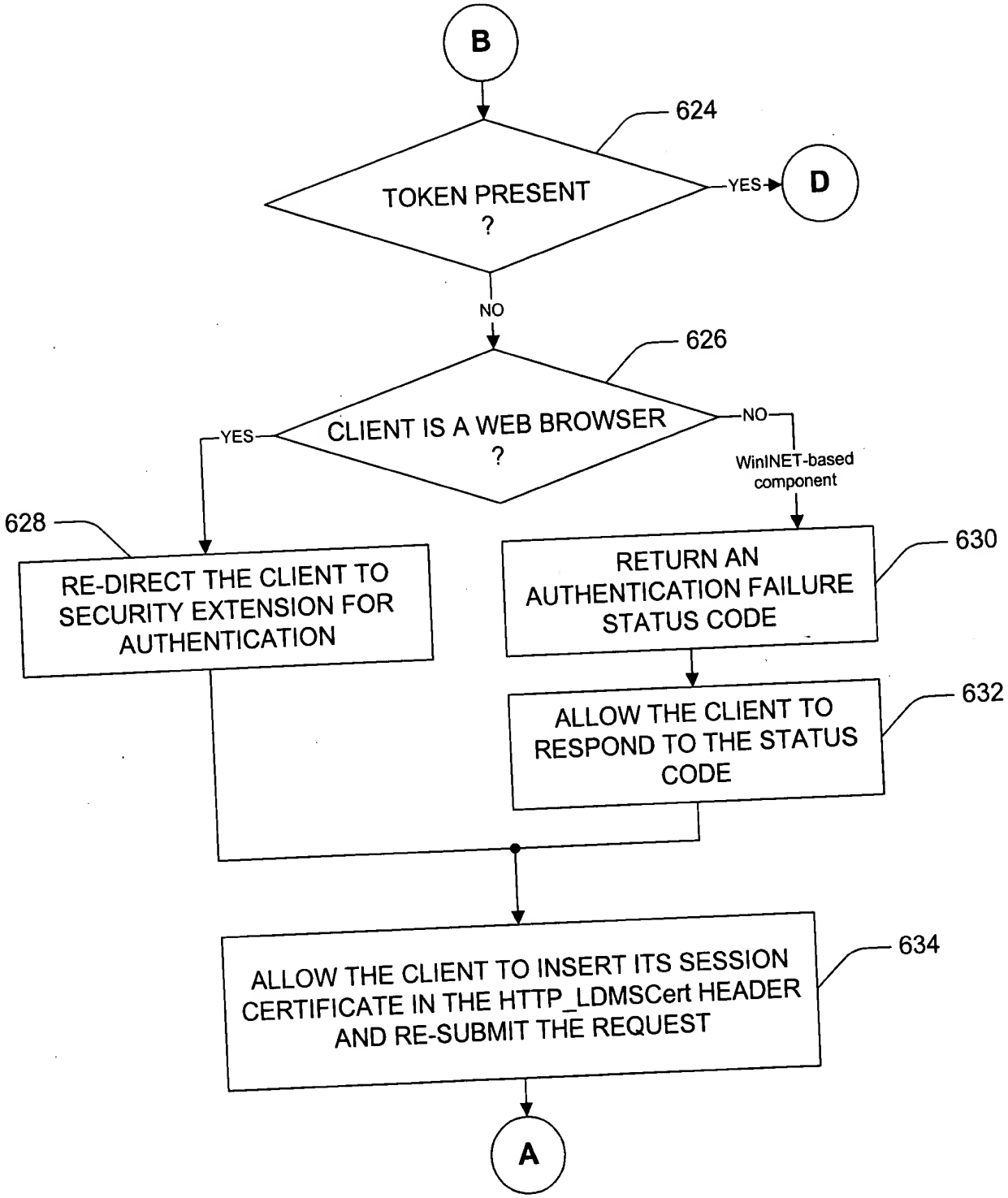
B
624
TOKEN PRESENT ?
YES
D
NO
626
CLIENT IS A WEB BROWSER ?
YES
NO
WinINET-based component
628
RE-DIRECT THE CLIENT TO SECURITY EXTENSION FOR AUTHENTICATION
RETURN AN AUTHENTICATION FAILURE STATUS CODE
630
ALLOW THE CLIENT TO RESPOND TO THE STATUS CODE
632
ALLOW THE CLIENT TO INSERT ITS SESSION CERTIFICATE IN THE HTTP_LDMSCert HEADER AND RE-SUBMIT THE REQUEST
634
A

FIG. 6C

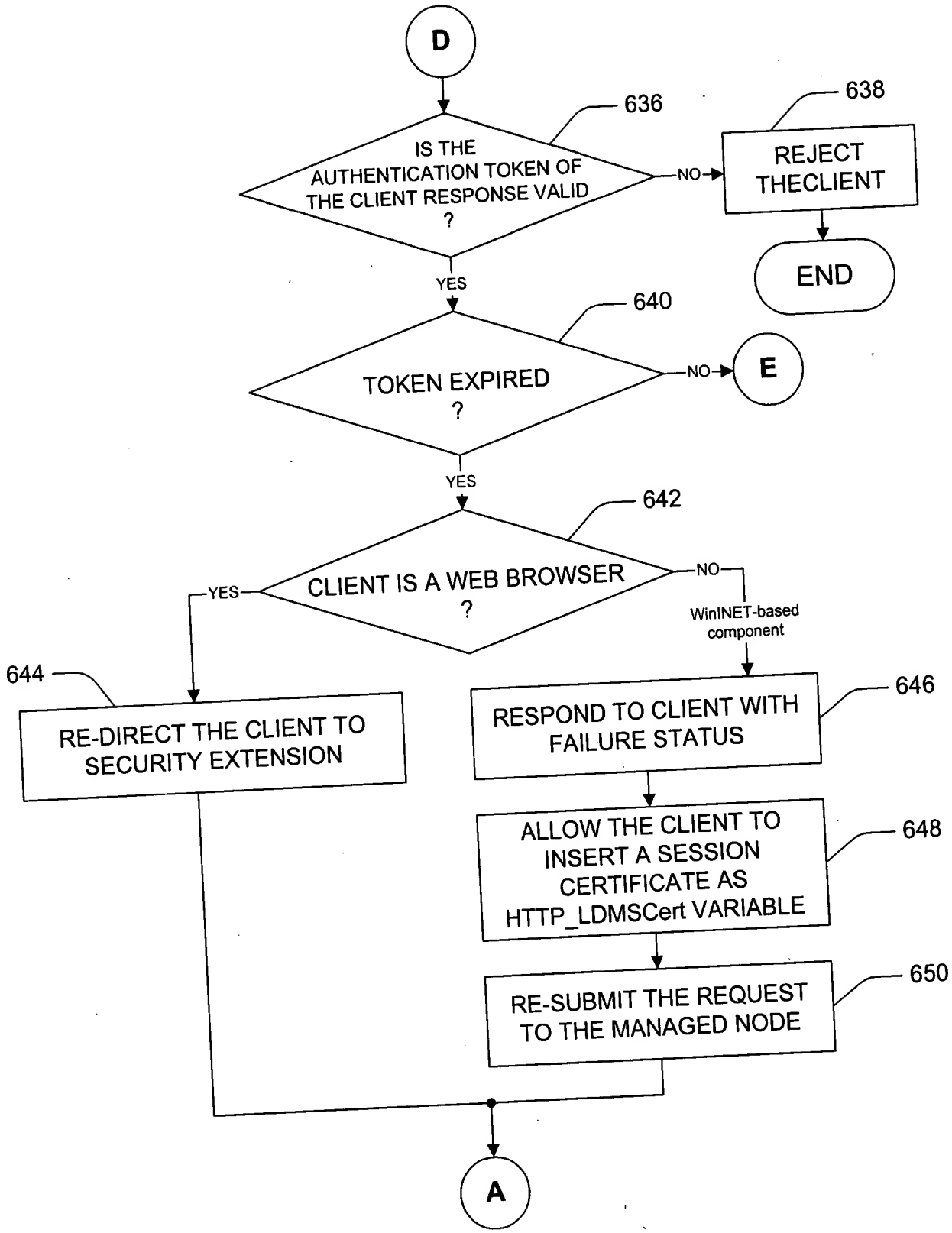
D
636
IS THE AUTHENTICATION TOKEN OF THE CLIENT RESPONSE VALID ?
NO
638
REJECT THECLIENT
END
YES
640
TOKEN EXPIRED ?
NO
E
YES
642
CLIENT IS A WEB BROWSER ?
YES
NO
WinINET-based component
644
RE-DIRECT THE CLIENT TO SECURITY EXTENSION
646
RESPOND TO CLIENT WITH FAILURE STATUS
ALLOW THE CLIENT TO INSERT A SESSION CERTIFICATE AS HTTP_LDMSCert VARIABLE
648
RE-SUBMIT THE REQUEST TO THE MANAGED NODE
650
A

FIG. 6D

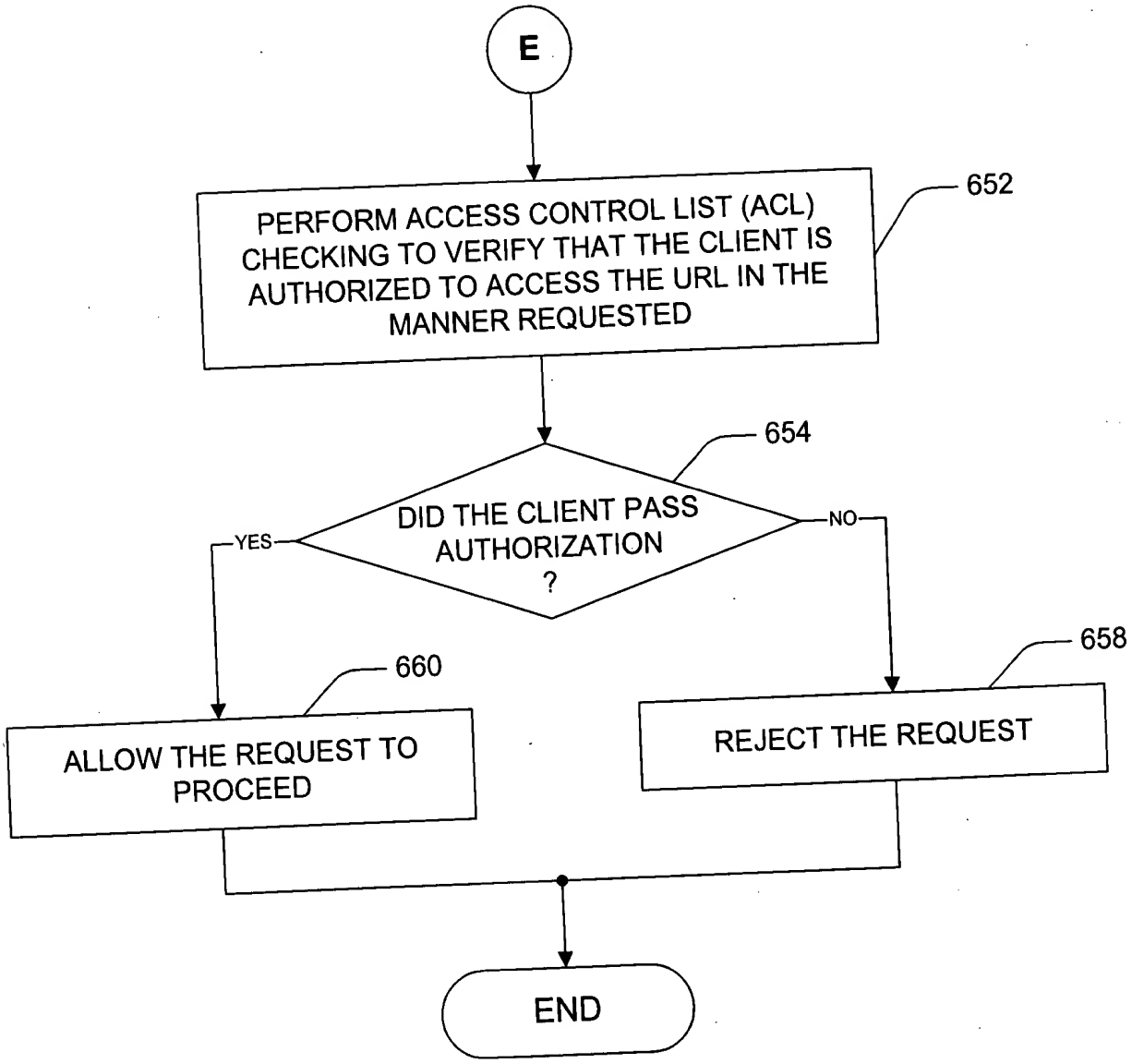
E
PERFORM ACCESS CONTROL LIST (ACL) CHECKING TO VERIFY THAT THE CLIENT IS AUTHORIZED TO ACCESS THE URL IN THE MANNER REQUESTED
652
DID THE CLIENT PASS AUTHORIZATION ?
654
YES
NO
ALLOW THE REQUEST TO PROCEED
660
REJECT THE REQUEST
658
END

FIG. 6E

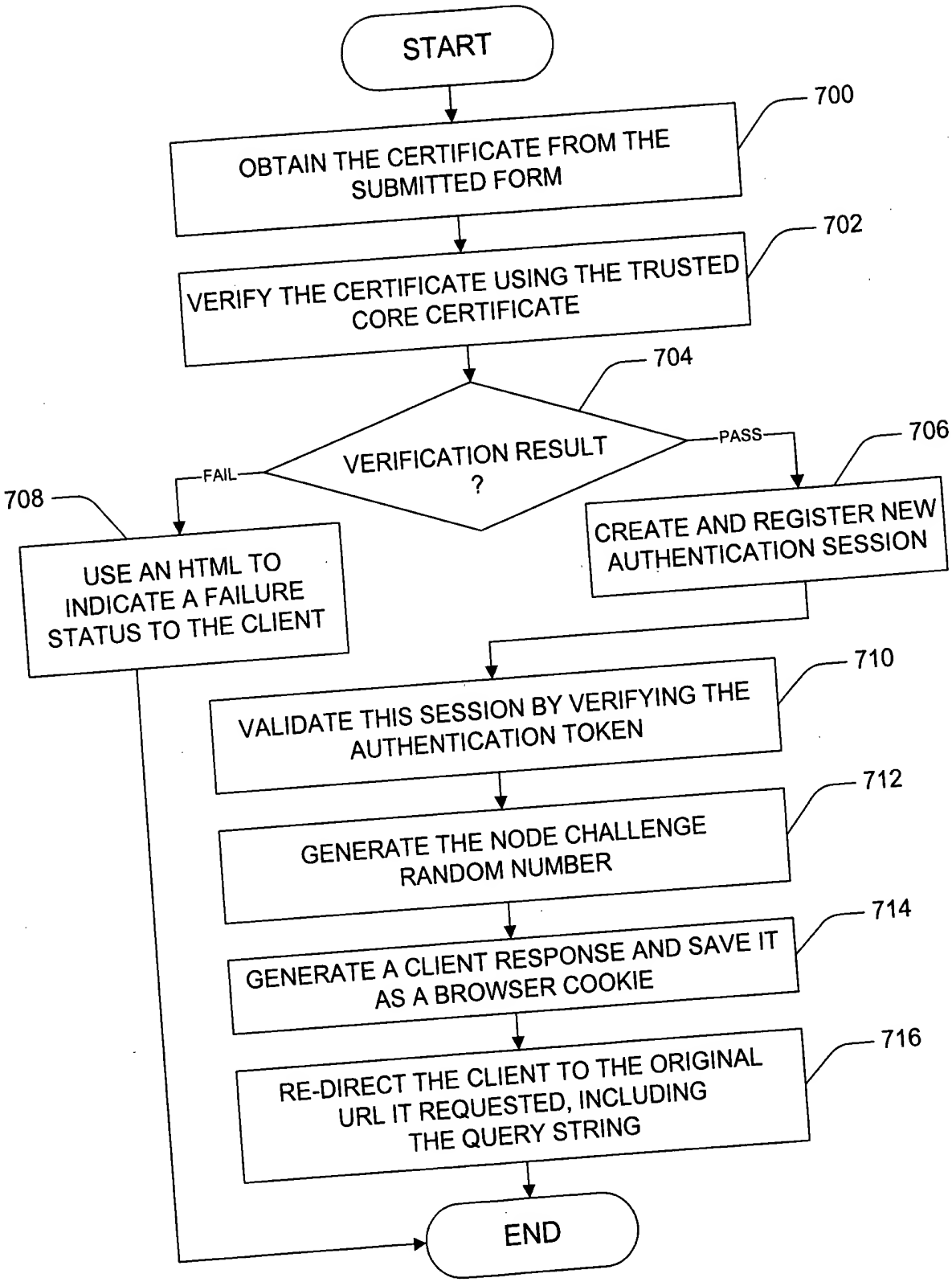
START
OBTAIN THE CERTIFICATE FROM THE SUBMITTED FORM
700
VERIFY THE CERTIFICATE USING THE TRUSTED CORE CERTIFICATE
702
VERIFICATION RESULT ?
704
PASS
FAIL
706
CREATE AND REGISTER NEW AUTHENTICATION SESSION
708
USE AN HTML TO INDICATE A FAILURE STATUS TO THE CLIENT
VALIDATE THIS SESSION BY VERIFYING THE AUTHENTICATION TOKEN
710
GENERATE THE NODE CHALLENGE RANDOM NUMBER
712
GENERATE A CLIENT RESPONSE AND SAVE IT AS A BROWSER COOKIE
714
RE-DIRECT THE CLIENT TO THE ORIGINAL URL IT REQUESTED, INCLUDING THE QUERY STRING
716
END

FIG. 7